Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Promoting Technological Solutions To	)	GN Docket No. 13-111
Combat Contraband Wireless Device	)	
Use in Correctional Facilities	)	FCC 17-25
	)	

CELL COMMAND, INC.'S REPLY COMMENTS
IN RESPONSE TO THE COMMISSION'S
FURTHER NOTICE OF PROPOSED RULEMAKING

Cell Command, Inc. ("Cell Command")[1], by and through its attorneys, respectfully submits these Reply Comments in connection with the Commission's May 18, 2017 Further Notice of Proposed Rulemaking ("*FNPRM*") and request for additional comments in the above-referenced proceeding. *See* 82 Fed. Reg. 22780 (May 18, 2017).

INTRODUCTION

The purpose of this proceeding is to identify a comprehensive technological solution to the growing and widespread threat to public safety propagated by the unlawful use of contraband wireless devices within the walls of U.S. correctional facilities. *See FNPRM* at Summary ("The Commission seeks comment on additional methods and technologies that might prove successful in combatting contraband device use in correctional facilities . . .). As the comments throughout this proceeding have made clear, the corrections and law enforcement communities – who are on the front lines of this daily fight – require a solution that is (1) comprehensive (i.e., "bricks the phone"), (2) cost effective (affordable for all correctional facilities), and (3) has minimal obsolescence (i.e., industry advancements must not hinder the system). As demonstrated below,

[1] Cell Command was formerly known as Try Safety First.

the comments submitted by representatives of these communities strongly support continuous wave beacon technology ("CW beacon") as that solution. Providers of contraband interdiction systems ("CISs") to correctional facilities also voice their support for CW beacon technology.

Moreover, the comments submitted in response to the *FNPRM* confirm what Cell Command demonstrated in its initial comments: that Managed Access Systems ("MAS"), jamming and geo-fencing, and the proposed detect-and-terminate regime envisioned by the *FNPRM* are not effective, affordable, viable or comprehensive solutions.

DISCUSSION

I. THERE IS SIGNIFICANT SUPPORT FOR CW BEACON TECHNOLOGY FROM THE CORRECTIONS COMMUNITY AND THE INDUSTRY

The American Correctional Association ("ACA"), which represents the interests of over 18,000 members of the correctional community in the United States and 900 correctional facilities, recommends that the adopted solution must (1) render the device completely unusable, (2) work on all devices, (3) be cost-effective, (4) not interfere with communications outside of the correctional facility, (5) be easy to implement and operate, (6) be secure, and (7) be legally compliant. *See* American Correctional Association Comments on Combating Contraband Wireless Device Use in Correctional Facilities (filed June 23, 2017) ("ACA 2017 Comments"), at 2-3. "ACA has reviewed the available technologies and finds that continuous wave beacon technology (CW beacon systems) meets all of the requirements and is especially attractive because it is cost-effective and does not require a huge capital expense." *Id.* at 3.

"CW beacon systems operate without interference with any cellular network frequencies, do not require human intervention by either corrections personnel or carrier personnel and can shut down ***all functions*** of the cell phone as soon as it picks up the signal from the beacon." *Id.* (emphasis original). Further, "[c]arrier and cell phone manufacturer involvement would be limited

to an initial push of the beacon technology onto cell phones on each carrier's respective network." *Id.* "After that, the continuous wave beacon technology would operate without any further involvement from the carrier or cell phone manufacturer, and could be automatically updated ensuing forward compatibility in the future." *Id.* "Anyone that tries to move or tamper with the beacon will render it unusable" and cause "its software to be wiped so that it cannot be reversed engineered." *Id.* Equally important, "[t]he cost of the beacons is minimal compared to every other system proposed for combating contraband cell phones." *Id.* For these reasons, ACA "believes that continuous wave beacon technology . . . incorporates all of" the features of a comprehensive, cost-effective solution (*id.*), and ACA strongly encourages the Commission to "gather the carriers and reach a voluntary agreement within one year to implement and offer CW beacon systems on all cell phones with a phase-in period of two years from the date of the agreement." *Id.* at 4.

The Association of State Correctional Administrators – whose "members lead over 400,000 correctional professionals and approximately 8 million inmates, probationers, and parolees" (*see* http://www.asca.net/ (last accessed July 17, 2017)), similarly supports the use of continuous wave beacon technology to combat the significant contraband wireless device public safety threat. *See* May 30, 2017 Comments of the Association of State Correctional Administrators, at 2 ("I am hopeful that you will consider requiring that wireless carriers cooperate and participate in the development of beacon technology, as referenced in your proposed rule. … [T]his technology would use software embedded in phones to provide a 100% solution, while allowing 'whitelisting' by correctional agencies as appropriate.").

In addition to representatives of the correctional community, CIS providers to that community also indicate support for beacon technology. Global Tel*Link Corporation – a provider of inmate calling services that "has been involved directly in the development and

provision of managed access systems ('MAS'), Contraband Interdiction Systems ('CIS'), and other techniques to deter the use of contraband wireless devices in the correctional facility environment" (June 19, 2017 Comments of Global Tel*Link Corporation, at 2) – supports the use of beacon technology (as well as other techniques) as an effective solution to the contraband cell phone public safety threat. *See id.* at 5-6. Similarly, ShawnTech Communications Inc., also a provider of inmate telephone systems and CISs (*see* http://www.shawntech.com/ (last accessed July 13, 2017)), recommends beacon systems as "one possible method of addressing [contraband wireless devices] in the [correctional facility] environment." *See* June 19, 2017 Comments of ShawnTech Communications Inc., at 5.[2]

Members of the carrier community – CTIA, T-Mobile, AT&T Services, Inc. and Verizon – submitted comments indicating opposition to beacon technology. Specifically, CTIA asserts that "dictating use of a beacon system that would require software embedded in wireless devices . . . would be a dramatic departure from the Commission's long-standing policy to remain technology-neutral and it would involve a sweeping government mandate." Comments of CTIA (June 19, 2017), at 9-10. T-Mobile makes the same argument. *See* Comments of T-Mobile USA, Inc. (June 19, 2017), at 18 ("Adoption of a rule requiring the use of this solution would be inconsistent with the Commission's policy against choosing technological winners and losers and would not promote technological neutrality."). CTIA and T-Mobile misunderstand Cell Command's position and that of the other commenters supporting beacon technology. While it is true that beacon

[2] Inpixon, a provider of detect-and-locate technology to correctional facilities, correctly recognizes that "tech-savvy inmates can and do utilize Wi-Fi, Bluetooth, and other wireless standards to operate contraband wireless devices. For that reason, Inpixon urges the Commission to pursue technical and regulatory solutions which address the full spectrum of contraband wireless communications – not just CMRS usage." Comments of Inpixon (June 19, 2017), at 2. Similarly, CellBlox, a provider of enhanced MAS, "strongly believes that service to contraband wireless devices that are detected should be terminated entirely and such devices should be rendered totally unusable." Initial Comments of CellBlox Acquisitions, LLC (June 19, 2017), at 3. As demonstrated by Cell Command and other commenters, CW beacon technology is the only technology that completely disables all functionality of all contraband wireless devices.

technology requires wireless device manufacturers to install a small data file along with the other software loaded onto newly-manufactured devices or via an over-the-air update for existing devices, correctional facilities would remain free to use whatever contraband interdiction system they choose or none at all. There is no request for a mandate to *use* beacon technology, only a request that the Commission adopt a voluntary program under which the wireless industry installs the software for beacon technology on wireless devices in order to permit correctional facilities – which support beacon technology in this proceeding – the *ability to use* such technology to ubiquitously and completely solve the contraband wireless device problem in a cost effective manner.

T-Mobile also contends that Cell Command's solution "will not cure the contraband phone problem" but "merely encourage the use of phones without the TSF software." Comments of T-Mobile USA, Inc. (June 19, 2017), at 19. Specifically, T-Mobile asserts that, even "[i]f the FCC requires all handsets operating or manufactured for sale in the U.S. to have the necessary software, a cottage industry will be created where handsets manufactured for sale overseas are smuggled into prison." *See id.*[3] However, T-Mobile is not aware of the technological capabilities of Cell Command's CW beacon technology (known as Cell Warden). Subsequent to the end of the migration period, Cell Command's CW beacon technology is designed to require the automatic, over-the-air installation of the software on any wireless device within the range of its hardware units the instant the device is powered on or comes within the range of the hardware. In other words, if a wireless device without the software protocol manufactured for sale overseas is smuggled into a correctional facility, the user of that device will receive a message when the device

[3] Verizon makes a similar argument. *See* Comments of Verizon (June 19, 2017), at 13 ("Beacon-based solutions are dependent not only on the capabilities of devices and the ability of OEMs to integrate the relevant hardware and software capabilities into their products, but the ubiquity of capable devices (*and the absence of non-capable devices*) among users . . .") (emphasis added).

comes within the range of the CW beacon hardware informing them that the software protocol must be downloaded over-the-air in order for the device to function or, alternatively, the user may purchase a protocol-enabled SIM card at a local retailer or communication store in order for the device to function. If the user elects not to install the software protocol, all functionality (except for 911 access) will be completely disabled.

CTIA also summarily asserts – without any support – that beacon technology would be "ineffective, burdensome, and costly, with a lengthy implementation process." Comments of CTIA (June 19, 2017), at 10. This assertion is factually incorrect on all accounts. Beacon technology is the ***only*** completely effective solution that can disable *all* functionality of *all* wireless devices. From the standpoint of the carriers, implementation can be as simple as any system update that a carrier routinely pushes out. New phones could have the software installed by the Original Equipment Manufacturer. Significant implementation, therefore, can occur within months, and nearly all cell phones could have the protocol within twenty-four months.

Further, as Cell Command's initial comments demonstrate, the cost of its beacon system (Cell Warden) will be eminently affordable and efficiently implemented for all correctional facilities. *See* Cell Command, Inc.'s Comments in Response to the Commission's Further Notice of Proposed Rulemaking (filed June 19, 2017), at 18. Once installed, there is minimal to no burden on the correctional facility, as all monitoring is conducted offsite. It is, quite literally, a set it and forget it solution.

CTIA also contends – again without any support – that beacon technology "would pose a cybersecurity threat to public safety by introducing a nationwide capability that could be used to block legitimate calls." Comments of CTIA (June 19, 2017), at 10. T-Mobile makes the same argument, also without any support. *See* Comments of T-Mobile USA, Inc. (June 19, 2017), at 18

(adoption of beacon technology "would also create the risks of privacy, security, and 'mission creep' – terminating service to phones in contexts outside the clearly warranted case of contraband devices . . .). This position, too, is factually incorrect and demonstrates a fundamental misunderstanding of how beacon technology works in general and how Cell Command's system works specifically. Beacon technology is only capable of disabling wireless devices within a given range of the hardware component that broadcasts the disabling signal within the correctional facility. *See* Cell Command, Inc.'s Comments in Response to the Commission's Further Notice of Proposed Rulemaking (filed June 19, 2017), at 17. With respect to Cell Command's Cell Warden system, this range is between one (1) to twenty (20) meters. *See id.* These hardware devices are strategically placed inside the prison fences and buildings to broadcast the signal, with all functionality – except 911 capabilities – of all wireless devices with the beacon software being disabled once inside the prison fence line and in range of the broadcast trigger signal. *See id.* The hardware that broadcasts the signal is not capable of "mission creep," as T-Mobile surmises, nor is it capable of blocking legitimate calls "nationwide," as CTIA speculates. Moreover, as Cell Command established, its Cell Warden beacons are tamper-proof and, if moved without authorization, an alert of attempted tampering is sent to the correctional facility and memory in the beacon is automatically wiped. *See id.* at 18. Simply put, there is no cybersecurity threat.

CTIA's final argument is that "there is a substantial question of whether mandating use of such technology would require Congressional legislation." Comments of CTIA (June 19, 2017), at 10. This is incorrect for two reasons. First, as demonstrated above, there is no request for a mandate that everyone use beacon technology. Second, as Cell Command's initial comments confirm, the Commission already has the authority under Section 332, Part 15 and its ancillary authority to ensure that all wireless carriers and wireless device manufacturers include beacon

software in wireless devices so that correctional facilities have the choice to use beacon technology to completely solve the contraband wireless device threat within their respective walls. *See* Cell Command, Inc.'s Comments in Response to the Commission's Further Notice of Proposed Rulemaking (filed June 19, 2017), at 19-26.

II. THE COMMENTS CONFIRM THAT OTHER PROPOSED SOLUTIONS ARE INEFFECTIVE

In its initial Comments, Cell Command demonstrated that Managed Access Systems ("MAS"), jamming and geo-fencing technologies, and the detect-and-terminate regime envisioned by the *FNPRM* are not viable solutions because, *inter alia*, these systems: (1) are not comprehensive and ubiquitous (i.e., they do not "brick" the device); (2) are expensive (too expensive to have more than a marginal local effect); (3) require significant oversight by the Commission, carriers, and/or correctional facility personnel; (4) are highly likely to create external interference issues; and/or (5) are illegal. *See* Cell Command, Inc.'s Comments in Response to the Commission's Further Notice of Proposed Rulemaking (filed June 19, 2017), at 7-16. The comments filed by several entities only confirm that these solutions are ineffective.

A. The Comments Demonstrate that MAS Systems are Not Viable Solutions

Prelude Communications, a CIS developer, indicates that, "[u]ntil recently, [it] believed that a MAS/CIS solution can and would be the best for all stakeholders." Prelude Communications Comments (filed May 1, 2017), at 2. However, "[w]ith the disappointing results and developments with MAS solutions deployed over the last 48 months and the lack of financial resources available by the correctional agencies, it has become clear, that a network based solution is required to provide an affordable alternative to MAS." *Id.* Indeed, as Cell Command discussed in its initial comments, the California Department of Corrections and Rehabilitation concluded that the Managed Access Systems it had installed in 18 of its facilities, while they blocked lots of calls,

were not blocking enough to justify the huge expense. *See* Cell Command, Inc.'s Comments in Response to the Commission's Further Notice of Proposed Rulemaking (filed June 19, 2017), at 9. In a meeting of the state correctional administrators at the FCC on June 29, 2017, the Secretary of the State of California's Department of Corrections, Scott Kernan, told Chairman Ajit Pai that the State of California would not be investing any money to install the upgrades required for the Managed Access Systems to continue working due to the millions of dollars it would cost and because of the disappointing performance. *See* Cell Command, Inc. *Ex Parte*, June 30, 2017. In essence, California is abandoning MAS.

GTL, another CIS provider which has been involved in implementing MAS systems in correctional facilities, similarly emphasizes that the cost of such systems render them an infeasible solution for all correctional facilities:

> MAS may be a cost-prohibitive solution for a facility given the complex technical components and staggering costs needed to deploy the system. Depending on the size of the facility, the number of sites within a facility complex, the surrounding geography from a topographical and urban versus rural standpoint, the architectural structure of the facility, and the ongoing system maintenance and software upgrades, costs to deploy MAS can start at $1.5 million or more per facility, and will continue to grow over time to cover costs related to system upgrades and maintenance. This does not include any of the regulatory costs for authority to operate such systems. While the Commission has streamlined the licensing process to some extent, it remains overwhelming and costly for many correctional facilities to implement.

See June 19, 2017 Comments of Global Tel*Link Corporation, at 3-4.

Inpixon, a detect-and-locate provider, correctly asserts that a system that only impacts communications on CMRS – like MAS – is inadequate because inmates can use non-CMRS technologies such as WiFi to access the internet to communicate with co-conspirators, thereby opening "a whole world of possibilities . . . to the enterprising inmate." June 19, 2017 Comments

of Inpixon, at 7. "Similarly, Bluetooth technology can be used to connect to other communication devices, to transfer files, to control [Internet of Things] technologies, and to tether to other devices." *Id.*

ACA indicates that while it "has supported the use of Managed Access Systems, having seen some of the problems with implementation, effectiveness, cost and issues with overbreadth and gaps, [ACA] discourage[s] the Commission from viewing managed access as the best solution or the final solution to solving this problem." ACA 2017 Comments, at 3. "MAS systems have their limitations and are very expensive to implement on a broad scale." *Id.* "More importantly, MAS does not necessarily disable all functions of a contraband cell phone that can be used to communicate with others," as "[c]ertain functions (e.g., camera usage and, potentially, internet access) may still be used by inmates." *Id.* at 4.

The Tennessee Department of Corrections similarly – and succinctly – summarizes the fatal flaws inherent in MAS systems that cannot be overcome by the streamlined application process envisioned by the Commission:

> Currently, managed access solutions are complicated and expensive to implement with costs exceeding one million dollars per site and are ineffective. Streamlining the application process is appreciated, however, the cost of licensing represents a very small percentage of the total cost and managed access is both easily defeated and an 'after the fact' solution.

Comments of the Tennessee Department of Correction (June 13, 2017), at 5.[4]

[4] The comments submitted by T-Mobile, Verizon, and AT&T all generally support MAS over other proposals and discuss purportedly successful spectrum lease negotiations with MAS providers and/or actual MAS rollouts at correctional facilities. *See* Comments of Verizon (June 19, 2017), at 3-4; Comments of T-Mobile USA, Inc. (June 19, 2017), at 1-2; Comments of AT&T Services, Inc. (June 19, 2017), at 3-4. Cell Command applauds these efforts, as correctional facilities should be free to adopt whichever contraband interdiction system they choose, including MAS *or* beacon technology. However, the fact that a few correctional facilities can afford MAS systems does not mean that all of them can, as this record vigorously demonstrates. Moreover, no matter how many traditional MAS systems are implemented, the fact remains that they are not capable of completely disabling all functionality of all wireless devices. At best, MAS systems present only a small speedbump to the contraband wireless device problem; they cannot stop the problem in its tracks.

B. The Comments Demonstrate that Jamming Systems are Not Viable Solutions

The ACA correctly asserts that "[j]amming systems can be over-inclusive and interfere with legitimate wireless devices in the surrounding areas." ACA 2017 Comments, at 4. "ACA has supported jamming systems, but it is [its] understanding that the FCC's position remains that jamming is banned statutorily." *Id.* "As with MAS, jamming systems still permit inmates to use certain functions on a contraband cell phone." *Id.* The same fatal flaw is inherent in Geolocation-Based Denial technology. *See id.*

The comments filed in support of jamming technology only highlight these same limitations, confirming that jamming technologies are only effective at interfering with cellular signals. *See e.g.* Comments of the Tennessee Department of Correction (June 19, 2017), at 5 ("Jammers prevent any communications *over the cellular network*, preventing even short duration communications from occurring.") (emphasis added); June 13, 2017 Comments of Global Tel*Link Corporation, at 8 ("Jamming technology is an effective tool for stopping unauthorized *wireless signals*, and when engineered properly, it does not raise issues for legitimate wireless users.") (emphasis added).

Even if jamming technology is used, other functions of a contraband wireless device (e.g., WiFi, camera, voice recording, notepad capability) can still be used by an inmate to communicate with a co-conspirator in furtherance of a criminal enterprise, rendering jamming an inviable solution.

C. The Comments Demonstrate that the Proposed Detect-and-Terminate Regime Envisioned by the *FNPRM* is Not Technologically Feasible

In the *FNPRM*, the Commission unequivocally states that it is "seek[ing] to ensure that any disabling process will *completely disable* the contraband device itself and render it unusable, not

simply terminate service to the device as the Commission had originally proposed in the" initial May 1, 2013 Notice of Proposed Rulemaking, FCC 13-58, 78 Fed. Reg. 36469. *See FNPRM* ¶ 19 (emphasis added). The comments demonstrate that the proposed detect-and-terminate program envisioned by the *FNPRM* is not capable of accomplishing this objective.

Indeed, Verizon confirms that it has extremely limited capability of disabling *all* functionality of *all* wireless devices operating on its cellular network:

> But the ability to fully and remotely 'disable' and 're-enable' a handset by disabling or locking it entirely (as is possible for some devices under the wireless industry's efforts to mitigate device theft) is currently limited to certain smartphone models and not available for feature phones and other connected devices.

See Comments of Verizon (June 19, 2017), at 9. T-Mobile confirms this limited capability as well. *See* Comments of T-Mobile USA, Inc. (June 19, 2017), at 2 n. 5 ("the record does not demonstrate that it is technically feasible and economically viable for CMRS carriers to completely disable alleged contraband devices . . .").

According to the carrier community, in order to completely disable a device, it is necessary for all devices to have software installed with the operating system:

> [A] licensee cannot disable devices today based on the unique device identifiers visible to the licensee; *the disabling capability is instead tied to the user's account with the operating system provider (e.g., iOS or Android).* To achieve the Further Notice's proposed requirements, *a new disabling capability would be required for all connected devices.*

See Comments of Verizon (June 19, 2017), at 9 (emphasis added). This is precisely what Cell Command is proposing with respect to CW beacon technology.[5]

[5] The comments also highlight the problems caused by the administrative busy work, unpredictable decision-making, and time delays that would be inherent in any detect-and-terminate regime that Cell Command discussed in its initial comments (*see* Cell Command, Inc.'s Comments in Response to the Commission's Further Notice of Proposed Rulemaking (filed June 19, 2017), at 12-16), as well as the disagreement among the various entities as to how the proposed detect-and-terminate system should function. *Compare, e.g.,* Arizona Department of Corrections

CONCLUSION

For the reasons set forth herein, as well as in Cell Command's initial comments in response to the *FNPRM*, the Commission should designate CW beacon technology for combatting contraband wireless devices in prisons, finding that it is the only current comprehensive, ubiquitous solution to the contraband wireless device public safety threat. The FCC should request that carriers and wireless device manufacturers work together with the FCC on a voluntary basis to develop a regime for implementation of the technology within two (2) years from the date of issuance so that correctional facilities have the ability to use CW beacon technology to completely solve the significant public safety threat caused by contraband wireless devices.

Dated: July 17, 2017

Respectfully submitted,

__/s/__James Arden Barnett, Jr_____
James Arden Barnett, Jr., Esq.
Rear Admiral USN (Retired)

__/s/__Stephen R. Freeland_____
Stephen R. Freeland, Esq.

__/s/__Ian Volner_____
Ian Volner, Esq.

__/s/__Christopher Boone_____
Christopher Boone, Esq.

Venable LLP
600 Massachusetts Ave., NW
Washington, DC 20001
(202)-344-4000

Its Attorneys

Comments (April 18, 2017), at 1 ("If a correctional institution, or its designee, is notifying a carrier, it must be accepted that we know what must be done in our facility") *with* Comments of T-Mobile USA, Inc. (June 19, 2017), at 5 ("CMRS carriers should not be required to terminate service solely on the basis that a device was identified as 'contraband' by correctional facility staff or a CIS operator"; arguing that "the Commission should require a court order be obtained directing a wireless carrier to terminate service to alleged contraband devices."); *see also* June 19, 2017 Comments of ShawnTech Communications Inc., at 1-2 (Item 14) (proposing detailed geological survey and testing for termination validation). This provides an additional, independent reason why that proposed regime is not a viable solution.